Rzeczpospolita Kadry i płace
12.12.19 nr: 289 str. 6 nakład: 55000 egz.

ZWOLNIENIA

Poufność informacji nie zależy od objęcia ich tajemnicą przedsiębiorstwa

Transferowanie dokumentów pracodawcy z jego serwera na prywatną pocztę elektroniczną pracownika należy kwalifikować w kontekście naruszenia podstawowych obowiązków pracowniczych nie tylko przez pryzmat tajemnicy przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, ale także, czy zawarte w nich informacje są tego rodzaju, że ich ujawnienie mogłoby narazić pracodawcę na szkodę, stwarzając potencjalną możliwość wykorzystana ich przez podmiot konkurencyjny.

PAWEŁ SYCH

Tak uznał **Sąd Najwyższy w wyroku z 3 kwietnia 2019 r. (II PK 334/17).**

Pracownica tuż przed złożeniem wypowiedzenia umowy o pracę przesłała na swój prywatny adres e-mail bazę danych potencjalnych klientów firmy. Pracodawca po uzyskaniu o tym wiedzy w czasie okresu wypowiedzenia, rozwiązał z nią umowę dyscyplinarnie. Jako przyczynę wskazał przesłanie na prywatną skrzynkę mailową bazy klientów, która była objęta tajemnicą przedsiębiorstwa.

Pracownica odwołała się od zwolnienia dyscyplinarnego. Sąd I instancji oddalił powództwo, wskazując, że zwolnienie w tym trybie było zasadne. Ocenił, że przesyłając bazę na prywatny adres kobieta naruszyła podstawowy obowiązek pracownika poprzez niezachowanie w tajemnicy informacji pracodawcy.

Powódka wniosła apelację od tej części wyroku, wskazując, że baza danych nie stanowiła tajemnicy przedsiębiorstwa, więc nie było obowiązku zachowania jej w poufności. Sąd II instancji uwzględnił apelację i uznał, że zwolnienie dyscyplinarne było nieuzasadnione. Wskazał, że pracownica nie naruszyła tajemnicy przedsiębiorstwa, gdyż baza danych nie spełniała definicji zawartej w ustawie o zwalczaniu nieuczciwej konkurencji. Ponadto sporządziła ją sama powódka na podstawie informacji ogólnodostępnych w internecie. Ponieważ baza klientów zawierała dane, które były dostępne w internecie, w ocenie sądu tych informacji nie można uznać za tajemnicę przedsiębiorstwa, a co za tym idzie – pracownica nie miała obowiązku zachowania ich w poufności.

Były pracodawca wniósł do SN skargę kasacyjną, zarzucając sądowi II instancji nieprawidłowe ograniczenie obowiązku pracownika do zachowania w poufności jedynie tajemnicy przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji. SN wskazał, że obowiązki pracownicze w tym zakresie dotyczą wszystkich informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, stwarzając chociażby potencjalną możliwość wykorzystania ich przez podmiot konkurencyjny. Uchylił zaskarżony wyrok w tym zakresie i przekazał sprawę do ponownego rozpoznania. /®

KOMENTARZ EKSPERTA

Paweł Sych

radca prawny w kancelarii Raczkowski Paruch w biurze w Katowicach

MAT. PRAS.

Nie ulega wątpliwości, że zachowanie w tajemnicy informacji pracodawcy należy do podstawowych obowiązków pracownika. To konkretyzacja ogólnego obowiązku dbania o dobro zakładu pracy i nienarażania interesu pracodawcy.

SN prawidłowo wskazał, że brak jest podstaw do ograniczenia obowiązku zachowania poufności jedynie do tajemnicy przedsiębiorstwa i obowiązek ten należy rozciągnąć na wszelkie informacje mogące nawet potencjalnie zagrażać interesom pracodawcy.

Tajemnica przedsiębiorstwa jest wyjątkowym rodzajem informacji, którą pracownik zobowiązany jest zachować w poufności. Podlegają one szczególnej ochronie nie tylko na podstawie kodeksu pracy, ale też ustawy o zwalczaniu nieuczciwej konkurencji, która ujawnienie, wykorzystanie lub pozyskanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa klasyfikuje jako czyn nieuczciwej konkurencji. Nie oznacza to jednak, że obowiązek ten nie dotyczy innych informacji.

W tej sprawie sąd II instancji stwierdził, że skoro baza zawierała dane kontaktowe ogólnodostępne w internecie, to nie jest ona objęta ochroną. Pominął przy tym, że o ile jednostkowe dane, które są ogólnodostępne, być może nie mają wartości dla pracodawcy i nie są objęte tajemnicą, to już ich zebranie i usystematyzowanie w bazie danych i powiązanie z informacją, że jest to np. baza klientów (faktycznych lub potencjalnych) nabiera znacznej wartości, a pracownik ma obowiązek ich nieujawniania. Dlatego SN słusznie wskazał, że nie stanowi to „zwykłego zbioru teleadresowego spółek", lecz jest informacją o szczególnym znaczeniu dla spółki. Co ważne, pracodawca w związku z niezachowaniem tajemnicy nie musi ponieść żadnej realnej szkody. Wystarczający jest fakt samej możliwości zagrożenia jego interesów w przyszłości. W związku z tym wszelkie przesyłanie danych pracodawcy, które mają dla niego wartość i których wykorzystanie może naruszyć jego interesy, na prywatne skrzynki mailowe czy kopiowanie ich na prywatne nośniki danych bez wyraźnego przyzwolenia pracodawcy, należy w mojej ocenie kwalifikować jako naruszenie podstawowych obowiązków pracowniczych. Ponadto to pracodawca, dla którego pracownik w ramach obowiązków zebrał informacje czy wytworzył bazę danych, jest ich dysponentem, który poniósł koszty z tym związane. Już z tego względu nie powinny ich wykorzystywać inne podmioty (w tym były pracownik) bez wyraźnej zgody.

Komentowana sprawa ujawnia jeszcze jeden istotny wątek związany z bezpieczeństwem informacji. Nawet jeżeli pracownik nie ma zamiaru wykorzystać informacji pracodawcy w sposób niezgodny z ich przeznaczeniem, to i tak jest zobowiązany korzystać z narzędzi, które gwarantują odpowiedni poziom zabezpieczenia danych. Dlatego też, jeżeli pracodawca lub przełożony wyraźnie tego nie zaaprobuje, każde kopiowanie na prywatne nośniki czy przesyłanie na prywatne skrzynki pocztowe rodzi ryzyko ich przypadkowej utraty i ujawnienia. Dotyczy to nie tylko informacji, które mają znaczenie gospodarcze dla pracodawcy, ale również wszelkich informacji zawierających dane osobowe, których zapewnienie bezpieczeństwa jest obowiązkiem pracodawcy i to na nim spoczywa odpowiedzialność w razie naruszenia ochrony danych osobowych. Doświadczenie pokazuje, że zgubienie prywatnego pendrive'a, czy uzyskanie dostępu do prywatnej skrzynki pocztowej przez osoby nieuprawnione, nie należy do rzadkości. Dlatego ważne jest zarówno wprowadzenie odpowiednich zasad czy polityk bezpieczeństwa danych i stanowcze ich przestrzeganie, jak również odpowiednie przeszkolenie w tym zakresie pracowników. /®